IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA
Harrisonburg Division

IN THE MATTER OF THE SEARCH OF: Information Associated with Google User codyreynolds136@gmail.com that is stored at Premises controlled by Google, LLC.	**UNDER SEAL** Case No. 5:20-mj-00041

AFFIDAVIT IN SUPPORT OF APPLICATION
FOR A SEARCH AND SEIZURE WARRANT

I, Brandon Smock, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant authorizing a search of the Google email account "codyreynolds136@gmail.com" (the "SUBJECT ACCOUNT") that is stored at premises owned, maintained, controlled, or operated by the company Google, LLC ("Google"), headquartered in Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), (b)(1)(A), and (c)(1)(A), to require Google to disclose to the government Google records and other information in its possession, including the contents of communications, pertaining to the subscriber or customer associated with the SUBJECT ACCOUNT.

2. I am a Special Agent with the U.S. Department of Homeland Security ("DHS"), Homeland Security Investigations ("HSI"), and have been employed by HSI since July 2019. As such, I have attended and graduated the Federal Law Enforcement Training Center Criminal Investigator Training Program as well as the HSI Special Agent training program. Prior to

becoming a Special Agent, I was a sworn Police Officer with Prince William County Police Department in Virginia since 2012. In the fall of 2016, I was transferred to Detective assigned to the Special Victim's Unit of the Prince William County Police Department Criminal Investigations Division. In the fall of 2017, I was assigned to the Northern Virginia/District of Columbia Internet Crimes against Children Task Force ("NOVA/DC ICAC"). Shortly after, I was sworn as a Special Police Officer with the Virginia State Police and later sworn as a HSI Task Force Officer. During the time as a Detective, I became a certified Child Forensic Interviewer, certified in forensic acquisition of digital evidence, as well as Peer-to-Peer investigations and Undercover Chat Concepts and Techniques. As part of my current duties as a HSI Special Agent, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal distribution, receipt, transportation, possession, and access with intent to view child pornography, in violation of 18 U.S.C. §§ 2252 and 2252A. I have received training in the area of child pornography and child exploitation and have observed and reviewed child pornography, as defined in 18 U.S.C. § 2256(8), numerous times in connection with my duties. Thus, due to my training and experience, I am able to identify child pornography when I see it. I have training and experience in the enforcement of the laws of the United States, including the preparation, presentation, and service of subpoenas, affidavits, criminal complaints, search warrants, and arrest warrants. As a federal agent, I am authorized to investigate violation of laws of the United States and, to execute warrants issued under the authority of the United States.

3. I am familiar with the information contained within this affidavit based upon the investigation I have conducted to date, which includes conversations with law enforcement officers and others, as well as review of reports and database records. This affidavit is intended to show

only that there is sufficient probable cause for the requested warrant and does not set forth all knowledge about this matter.

DEFINITIONS

4. The following definitions apply to this Affidavit and its Attachments:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other highspeed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices. *See* 18 U.S.C. § 1030(e)(1).

c. "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer or other digital device to access the Internet. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

d. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

CHARACTERISTICS OF INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN OR VISUAL DEPICTIONS OF CHILDREN

5. Based upon my training and experience, as well as upon information provided to me by other law enforcement officers, there are certain characteristics common to individuals who produce, distribute, receive, and/or possess child pornography, which may be exhibited in varying combinations:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children, from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses (such as in person, in photographs, or other visual media), or from literature describing such activity. Due to the accessibility and availability of child pornography on the Internet, in my recent experience, instead of maintaining collections, some offenders engage in a pattern of viewing or downloading child pornography online and then deleting the material.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. They may also use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe,

secure and private environment, such as a computer and surrounding area. These collections can be maintained for several years to enable the individual to view the collection, which is valued highly.

d. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

e. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

f. Individuals whose sexual interest in children or images of children has led them to purchase access to paid websites or other commercial sources of child pornography frequently maintain the financial records of those transactions at their residences.

THE INVESTIGATION

Background on Relevant Technology: Kik

6. Kik Messenger ("Kik") is a free mobile application designed for chatting or messaging that is owned and operated by Kik c/o MediaLab.AI Inc. (formally owned and operated by Kik Interactive, Inc.). Kik uses a mobile device's data plan or Wi-Fi to transmit and receive messages. According to the publicly available information, to use this application, a user

downloads the application to a mobile phone, computer, or other digital device via a service such as the iOS App Store, Google Play Store, Apple iTunes, or another similar provider. Once the application is downloaded and installed, the user is prompted to create an account and username. The user also creates a display name, which is a name that other users see when transmitting messages back and forth. Once the user has created an account, the user is able to locate other users via a search feature. While messaging, users can then send each other text messages, images, and videos. In or about 2019, Kik was acquired by MediaLab, a U.S. company that continues to operate the Kik messaging application.

Background on Relevant Technology: MEGA

7. MEGA is a cloud storage, file hosting and sharing website owned by Mega Limited, an Auckland, New Zealand-based company. MEGA is offered via web-based applications but also includes mobile applications for Windows Phone, Android, and iOS. MEGA is also known for its large fifty [50] Gigabyte storage allocation for free user accounts.

Background on Relevant Technology: Google

8. From my review of publicly available information provided by Google about its service, including Google's "Privacy Policy," I am aware of the following about Google and the information collected and retained by Google.

9. Google provides a variety of on-line services, including email access, to the general public. Google allows subscribers to obtain email accounts at the domain name "gmail.com," like the email account listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, e-mail addresses, and, for paying subscribers, a means and a source

of payment (including any credit or bank account number). Thus, the computers of Google are likely to contain stored electronic communications (including retrieved and un-retrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

10. In general, an email that is sent to a Google subscriber is stored in the subscriber's "mail box" on Google servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Google servers indefinitely.

11. Emails stored in a subscriber's mail box may contain information pertaining to new social media and/or cellular phone application accounts that were created, such as account activation emails that require verification to create new social media and/or cellular phone application accounts. Such account activation emails can indicate that the subscriber of the email account received notification and/or verified the creation of new social media and cellular phone application accounts such as Kik and MEGA. This is particularly important if such new social media and/or cellular phone application accounts were used to conduct illicit activities.

12. When the subscriber sends an email, it is initiated at the user's electronic device, transferred via the Internet to Google's servers, and then transmitted to its end destination. Google often saves a copy of the email sent. Unless the sender of the email specifically deletes the email from the Google server, the email can remain on the system indefinitely.

13. Subscribers to Google might not store on their home computers copies of the emails stored in their Google account. This is particularly true when they access their Google account through the web, or if they do not wish to maintain particular emails or files in their residence. A

Google subscriber can also store files, including emails, address books, contact or buddy lists, pictures, and other files, on servers maintained and/or owned by Google including updating many functions, applications, and drives on Google's cloud storage system, Google Drive.

14. Google Drive is a cloud storage and synchronization service developed by Google. Google Drive allows users to store files on its servers, synchronize files across devices, and share files. In addition to a website, Google Drive offers apps with offline capabilities for Windows and macOS computers as wells as Android and iOS smartphones and tablets. A person may sign up for Google Drive, Gmail, Google Photos, and other Google services by creating a Google account, which provides the account user with 15 gigabytes of free cloud storage. The Google Photos app automatically sends photos to Google Drive. The Google Photos app can also automatically delete photos on your phone that have already been uploaded to Google Drive. A Gmail user is able to store email attachments sent through Gmail directly to their Google Drive. In my training and experience I am aware people may save photographs received in email attachments to their cloud storage such as Google Drive. I am also aware that images of child pornography have been found in cloud storage such as Google Drive. This information may provide clues to the subscriber's identity, location, or illicit activities.

15. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contact lists,

and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). This geographic information may tend to either inculpate or exculpate the account owner. Last, stored electronic data may provide relevant insight into the email account user's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the user's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

16. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, cloud services (Google Drive) and attachments to e-mails, including pictures and files.

17. In addition, Google typically retains certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was crated, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the used to connect to the account, and other log files that reflect usage of the account. In addition, methods, providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help identify which computers or other devices were used to access the account. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Google subscribers) and information concerning subscribers

and their use of Google services, such as account access information, the email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

Probable Cause

18. HSI agents have determined that an individual, likely William Cody REYNOLDS, at 1527 Carpers Pike, Gore, Virginia 22637 has possessed and/or distributed images of child pornography using an electronic device, which may be associated with the SUBJECT ACCOUNT.

19. Specifically, according to an Investigator with the Frederick County Sheriff's Office ("FCSO"), he has investigated William Cody REYNOLDS for child exploitation offenses. That investigation stems from two National Center for Missing and Exploited Children ("NCMEC") CyberTips, received in February 2019, relating to a Dropbox, Inc. account. Specifically, the Dropbox, Inc. account contained approximately five hundred and thirty-seven (537) images and/or videos of suspected child pornography and was registered with the email address "codyreynolds119@gmail.com" between August 12, 2018 and October 10, 2018.

20. Through administrative subpoenas to Dropbox, investigators learned that the email address of "codyreynolds119@gmail.com" had an associated telephone number of 540-323-0524, which was owned by Verizon and assigned to REYNOLDS at 1527 Carpers Pike, Gore, Virginia 22637.

21. Based on this information, on or about May 2019, the FCSO Investigator executed a Virginia state search warrant at 1527 Carpers Pike, Gore, Virginia 22637. During that search, officers seized a LG Gpad X 8.0, Samsung Tablet, and a LG cellular telephone. Law enforcement subsequently searched the electronic devices, which yielded no child pornography material,

according to the FCSO investigator. Consequently, on or about June 3, 2019, the devices were returned to REYNOLDS, allowing him continued access to social media applications and electronic storage providers (e.g., Dropbox/MEGA) using the electronic devices.

22. In addition, during the execution of the search warrant, law enforcement conducted an interview with REYNOLDS, who was present at the time. REYNOLDS admitted being the owner of the previously-described Dropbox account as well as accessing the Kik chat groups where the child pornography was shared. REYNOLDS stated he would save the child pornography received from the Kik chat groups and upload the material into the Dropbox account for future access. REYNOLDS also explained that he had obtained a new cellphone, which may explain, in part, why the FCSO did not find child pornography evidence on those electronic devices.

23. Law enforcement arrested REYNOLDS, who is now charged in Frederick County, Virginia state court with one (1) count of Virginia Criminal Code 18.2-374.1 (Possess Obscene Material with Minor) and nine (9) counts of Virginia Criminal Code 18.2-374.1 (Child Pornography, Possess 2+ Offense). He was initially released on bond in that case, which is still pending.

24. In or about February 2020, an HSI Special Agent based in Blaine, Washington, was actively engaged in an online undercover operation on Kik. As part of the investigation, the HSI Special Agent had access to Kik chat groups, which engaged in the trading and distribution of child pornography.

25. In or about March 2020, a Kik user using the username "codman50" shared the following MEGA link in a group chat:[1] https://mega.nz/#F!hLIBTS6D!J_QeUrAT4k9KjoNHwDFCxw ("MEGA Link").

26. The HSI Special Agent was able to access and view the shared MEGA Link, which contained a folder titled "(1)" which in turn contained approximately 4.14 gigabytes of images and videos of child pornography. For example, the HSI Special Agent advised your affiant that one video depicts a young prepubescent male, approximately nine (9) years in age, performing fellatio on an adult, erect penis.

27. On or about April 1, 2020, HSI requested Kik business records associated with the Kik username "codman50." Kik provided records in response to the subpoena, which included the following:

> Kik Account: codman50_liu
> First Name: cody
> Last Name: reynolds
> Email: codyreynolds136@gmail.com (confirmed) (SUBJECT ACCOUNT)
> Username: codman50

28. On or about June 24, 2020, HSI requested Google Inc. business records for the email address of SUBJECT ACCOUNT which was used to register the Kik account of username "codman50." Google Inc. provided records in response to the subpoena, which included the following:

> Google Account ID: 208063747861
> Name: Cody Reynolds
> e-Mail: codyreynolds136@gmail.com
> Created on: 2015-11-13 23:08:13 UTC
> Last Logins: 2018-10-24 03:42:59 UTC, 2018-10-22 07:37:11 UTC, 2018-06-29 02:23:40 UTC

[1] Your affiant knows the name/title of the Kik group chat; however, to protect the confidentiality of ongoing investigations related to the same chat group, your affiant does not list it here.

Recovery SMS: +15403230542 [US]

29. An open source database identified the Google Account Recovery telephone number belonged to William C. REYNOLDS residing at 1527 Carpers Pike, Gore, Virginia 22637.

30. On or about July 9, 2020, your affiant attempted to view the shared MEGA link by "codman50." However, the link was no longer active and displayed a statement disclosing the following: "This folder/file was reported to contain objectionable content, such as Child Exploitation Material, Violent Extremism, or Bestiality…"

31. On or about July 10, 2020, your affiant requested assistance from the HSI Attaché in Canberra, New Zealand in reference to obtaining records/details of the MEGA link described in Paragraph 25 and the SUBJECT ACCOUNT from Mega Limited. HSI Canberra issued a subpoena to the New Zealand Department of Internal Affairs in accordance with previously established practices in reference to obtaining business records from Mega Limited. On or about July 13, 2020, the New Zealand Department of Internal Affairs advised that the SUBJECT ACCOUNT created/set-up a MEGA account on or about November 11, 2019 at 04:30:42 UTC, however the creator did not verify the account via the confirmation email. In addition, the contents of the MEGA link were provided, which included approximately three hundred and ninety-seven (397) media files, including but not limited to:

a. A video file titled "455.mp4" which depicts a pre-pubescent juvenile male wearing a red and white shirt. The juvenile is performing fellatio on a nude, adult male who is lying on his back.

b. A video file titled "354.mp4" which depicts an obese, Asian male wearing a red long-sleeved shirt, sitting on a black couch. There are two nude pre-pubescent males sitting in front of the adult male. One of the juveniles performs fellatio on

the adult. Later in the video, the adult begins kissing one of the boys as the other boy performs fellatio on him.

c. A video file titled "837.mp4" which depicts a nude adult male lying on a bed with a pre-pubescent male wearing blue shorts is manipulating the adult's penis. The juvenile begins to perform fellatio on the adult. Later in the video, the adult performs fellatio on the juvenile.

32. Therefore, there is probable cause to believe that the SUBJECT ACCOUNT contains evidence of the possession and/or distribution and/or receipt of child pornography, because REYNOLDS appears to be using the SUBJECT ACCOUNT to create other accounts from which he is storing or distributing child pornography.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

33. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular Title 18, United States Code, Sections 2703(a),(b)(1)(A), and (c)(1)(A), by using the warrants to require Google to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

34. Based on the information set forth above, I submit this affidavit supports probable cause to believe the SUBJECT ACCOUNT contains or constitute evidence, fruits, instrumentalities, and/or contraband related to violations of Title 18, United States Code, Section

2252. I therefore request the Court issue the proposed search and seizure warrant in order to seek the items described in Attachment B.

35. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

SEALING ORDER REQUESTED

36. It is respectfully requested that this Court issue an order sealing, until further order of this Court, all papers submitted in support of this application, including the application, affidavit, and search warrant, and the requisite inventory notice. Sealing is necessary because the items and information to be seized are relevant to an ongoing investigation, and premature disclosure of the contents of this Affidavit and related documents may jeopardize the effectiveness of the investigation.

OATH

The information in this affidavit is true to the best of my knowledge and belief.

Respectfully submitted,
s/Brandon Smock
Brandon Smock, Special Agent
Homeland Security Investigations

Received by reliable electronic means and sworn and attested to by telephone on this 25th day of August 2020.

JOEL C. HOPPE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be searched

This warrant applies to information associated with "codyreynolds136@gmail.com" that is stored at premises owned, maintained, controlled or operated by Google, LLC, which is headquartered in Mountain View, California.

ATTACHMENT B

Items to be seized

I. Information to be disclosed by Google LLC (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A.

a. The contents of all emails associated with the account **from January 1, 2019 through the date of the warrant is served**, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, long-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. All information regarding the particular device or devices used to login to or access the account, including all device identifier information or cookie information, including all information about the particular device or devices used to access the

account and the date and time of those accesses;

d. All data and information associated with the profile page, including photographs, "bios" and profile background and themes;

e. All location data associated with the account;

f. They types of service utilized;

g. All information about connections between the account and third-party websites and applications;

2. All records pertaining to devices from which the account accessed and Google services or which any Google service is synced, to include device serial numbers, model type/number, IMEI, and MAC address;

a. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

b. All records or other information, including images and videos, pertaining to Google Drive, Google Alerts, Google Chat Features, Google Contacts, Google Docs, Google Files Go, Google Groups, Google Meet, Google Photos, Google Hangouts, Google Hangouts Chat, Image search, Maps, Messages, Photoscan, Sheets, Google Voice.

c. Any accounts linked by hardware cookie to the account from January 1, 2019 through the date the warrant is served; and

d. All records pertaining to communications between the Provider and any person regarding the account including contacts with support services and records of actions taken.

The provider is hereby ordered to disclose the above information to the government within

14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of **18 U.S.C. §§ 2251 and 2252**, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Communications to and from Kik, MEGA, Dropbox, and other electronic services providers that can be used to receive, distribute, and possess child pornography.

(b) Possession, receipt, and production of child pornography;

(c) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the Google account owner;

(d) Evidence indicating the Google account owner's state of mind as it relates to the crime under investigation;

(e) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

(f) The identity of the person(s) who communicated with the user ID about matters relating to the receipt or distribution of child pornography, including records that help reveal their whereabouts.

(g) Information regarding the account holder's use of other electronic devices to access the Google account.

This warrant authorizes a review of electronically stored information, communication, other records and information disclosed pursuant to this warrant in order to located evidence, fruits, and instrumentalities described in the warrant. The review of this electronic data may be

conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, HSI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.